CLAIMS

What is claimed is:

1. A platform comprising:

a processor; and

a memory coupled to the processor, the memory including an isolated memory area containing a file checker executable by the processor, the file checker including (i) a file analyzer to perform a scan operation on a file to produce a scanning result and (ii) a signature generator to produce a digital signature chain including a digital signature having the scanning result.

2. The platform of claim 1, wherein the scan operation by the file checker is a virus detection function.

3. The platform of claim 1 wherein the incoming file is prevented from being executed if the verified digital signature chain indicated an unacceptable file integrity.

4. The platform of claim 1, wherein the incoming file is accessed if the verified digital signature chain indicates acceptable file integrity.

5. The platform of claim 1 further comprising a first control unit coupled to both the processor and the memory.

6. The platform of claim 5 further comprising a second control unit coupled to the first control unit and a token bus interface.

7. The platform of claim 6 further comprising a non-volatile memory coupled to the second control unit.

8. The platform of claim 6 further comprising input/output devices coupled to the second control unit.

9. The platform of claim 2 wherein the file analyzer is one of a virus detector, an intrusion detector, and a file integrity checker.

10. The platform of claim 1 wherein the signature generator comprises:

an encryptor to encrypt the scanning result using a signature key; and

a time stamper coupled to the encryptor to time stamp the encrypted result using a time indicator, the time stamped encrypted result corresponding to the digital signature.

11. The apparatus of claim 10 wherein the time indicator is one of a calendar time and a version identifier of the scanner.

12. The apparatus of claim 1 wherein the file is code.

13. A method comprising:

determining whether a digital signature chain accompanies a file to be accessed; and

verifying the digital signature chain of the file by determining (i) whether the file has an acceptable file integrity, and (ii) whether each signatory providing the digital signature chain is authorized.

14. The method of claim 13 further comprising:

precluding access to the file if the file has an unacceptable file integrity.

15. The method of claim 14 further comprising:

precluding access to the file if at least one signatory of the digital signature chain is unauthorized.

16. The method of claim 13, wherein prior to verifying the digital signature chain, the method further comprising:

entering into isolated execution mode if the file does not have a corresponding digital signature chain;

analyzing an integrity of the file; and

issuing the digital signature chain if the file has an acceptable file integrity.

17. The method of claim 16 further comprising:

issuing the digital signature chain with an indication that the file integrity is unacceptable if the integrity of the file is analyzed and determined to be unacceptable.

18. The method of claim 13 further comprising:

opening the file if the verified digital signature chain indicates an acceptable file integrity; and

refusing to open the file if the verified digital signature chain indicates an unacceptable file integrity.

19. A computer program embodied in a processor readable medium and executable by a processing unit, comprising:

code for determining whether a digital signature chain accompanies a file to be accessed; and

code for verifying the digital signature chain of the file by determining (i) whether the file has an acceptable file integrity, and (ii) whether each signatory providing the digital signature chain is authorized.

20. The method of claim 19 further comprising:

code for precluding access to the file if the file has an unacceptable file integrity.

21. The method of claim 19 further comprising:

code for precluding access to the file if at least one signatory of the digital signature chain is unauthorized.